The following security alert was issued by the Information Security Division of the Mississippi Department of ITS and is intended for State government entities. The information may or may not be applicable to the general public and accordingly, the State does not warrant its use for any specific purposes.

DATE(S) ISSUED:
1/19/2010

SUBJECT:
Vulnerability in Apple iTunes and Quick Time Could Allow For Remote Code Execution

OVERVIEW:
A vulnerability has been discovered in Apple iTunes and Quick Time player. Apple iTunes and QuickTime are used to play media files on Microsoft Windows and MAC OS X platforms. This vulnerability can be exploited if a user views the malicious file on a webpage or opens a malicious file, including an email attachment, using a vulnerable version of Apple QuickTime Player or iTunes. Successful exploitation could result in an attacker gaining the same privileges as the logged on user. Depending on the privileges associated with the user, an attacker could then install programs; view, change, or delete data; or create new accounts with full user rights. Failed exploit attempts will result in a denial-of-service condition.

It should be noted that there is no patch available for this vulnerability, and it is being actively exploited on the Internet.

SYSTEMS AFFECTED:

Apple iTunes 8.0.2 20 and earlier
Apple QuickTime Player 7.5.5 and earlier
Apple Mac OS X 10.3.9
Apple Mac OS X 10.4.9
Apple Mac OS X 10.5
Apple Mac OS X Server 10.3.9
Apple Mac OS X Server 10.4.9
Apple Mac OS X Server 10.5

RISK:

Government:
Large and medium government entities: **High**
Small government entities: **High**

Businesses:
Large and medium business entities: **High**
Small business entities: **High**

Home users: High

DESCRIPTION:
A vulnerability has been discovered in Apple iTunes and Quick Time player. This is a buffer-overflow vulnerability which is caused by the applications' failure to perform a bounds-check on user-supplied data before copying it into an insufficiently sized buffer. This vulnerability can be exploited if a user has a vulnerable version of Apple QuickTime or iTunes and opens a specially crafted QuickTime or iTunes file (.mov file extension), including an email attachment or views the malicious file on a webpage. Successful exploitation could result in an attacker gaining the same privileges as the logged on user. Depending on the privileges associated with the user, an attacker could then install programs; view, change, or delete data; or create new accounts with full user rights. Failed exploit attempts will result in a denial-of-service condition.

It should be noted that there is no patch available for this vulnerability, and it is being actively exploited on the Internet.

RECOMMENDATIONS:
The following actions should be taken:

- Consider blocking the .mov file extension at the network perimeter until patches can be applied.
- If Apple iTunes or Quick Time players are your default media player, consider changing the default to another media player.
- Do not open email attachments from unknown or un-trusted sources.
- Remind users not to visit un-trusted websites or follow links provided by unknown or un-trusted sources.
- Run all software as a non-privileged user (one without administrative privileges) to diminish the effects of a successful attack.

REFERENCES:

Security Focus:
http://www.securityfocus.com/bid/32540/info

SANS:
http://www.offensive-security.com/blog/vulndev/multiple-media-player-http-datahandler-overflow/

CVE:
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2008-5406

ISS:
http://xforce.iss.net/xforce/xfdb/46984

Juniper Networks:
http://www.juniper.net/security/auto/vulnerabilities/vuln32540.html